EXHIBIT M

Manual for BIG-IP® Application Security Manager™ (excerpt)

BIG-IP® Application Security Manager™: Implementations

Version 13.1

Table of Contents

Preventing DoS Attacks on Applications

What is a DoS attack?

A *denial-of-service attack (DoS attack)* or *distributed denial-of-service attack (DDoS attack)* makes a victim's resource unavailable to its intended users, or obstructs the communication media between the intended users and the victimized site so that they can no longer communicate adequately. Perpetrators of DoS attacks typically target sites or services, such as banks, credit card payment gateways, and e-commerce web sites.

Application Security Manager™ (ASM) helps protect web applications from DoS attacks aimed at the resources that are used for serving the application: the web server, web framework, and the application logic. Advanced Firewall Manager™ (AFM) helps prevent network, SIP, and DNS DoS and DDoS attacks.

HTTP-GET attacks and page flood attacks are typical examples of application DoS attacks. These attacks are initiated either from a single user (single IP address) or from thousands of computers (distributed DoS attack), which overwhelms the target system. In page flood attacks, the attacker downloads all the resources on the page (images, scripts, and so on) while an HTTP-GET flood repeatedly requests specific URLs regardless of their place in the application.

About recognizing DoS attacks

Application Security Manager™ determines that traffic is a DoS attack based on calculations for transaction rates on the client side (TPS-based) or latency on the server side (stress-based). You can specify the thresholds that you want the system to use, or let the system automatically detect reasonable thresholds based on examining traffic patterns.

Note: *You can set up both methods of detection to work independently or you can set them up to work concurrently to detect attacks on both the client side and server side. Whichever method detects the attack handles DoS protection.*

You can also have the system proactively identify and prevent automated attacks by web robots. In addition, the system can protect web applications against DoS attacks on heavy URLs. Heavy URL protection implies that during a DoS attack, the system protects the heavy URLs that might cause stress on the server.

You can view details about DoS attacks that the system detected and logged in the event logs and DoS reports. You can also configure remote logging support for DoS attacks when creating a logging profile.

When to use different DoS protections

Application Security Manager™ provides several different types of DoS protections that you can set to protect applications. This table describes when it is most advantageous to use the different protections. You can use any combination of the protections.

DoS Protection	When to Use
Proactive bot defense	To stop DoS attacks before they compromise the system. Affords great protection and stops non-human traffic before it gets to ASM.

DoS Protection	When to Use
Bot signatures	To allow requests from legitimate (benign) bots, and instruct the system how to handle malicious bots (you can ignore, log, or block them). Logging malicious bots gives them visibility in the reports.
TPS-based detection	To focus protection on the client side to detect an attack right away, mostly by looking at the requests per seconds thresholds.
Stress-based detection	To focus protection on the server side where attacks are detected when a server slowdown occurs. This protection provides more accurate DoS detection based on latency and requests per second thresholds.
Behavioral detection	To use behavioral analysis and machine learning of traffic flows to automatically discover and mitigate DoS attacks.
Heavy URL protection	If application users can query a database or submit complex queries that may slow the system down.
CAPTCHA challenge	To stop non-human attackers by presenting a character recognition challenge to suspicious users.

About proactive bot defense

Application Security Manager™ (ASM) can proactively defend your applications against automated attacks by web robots, called *bots* for short. This defense method, called *proactive bot defense*, can prevent layer 7 DoS attacks, web scraping, and brute force attacks from starting. By preventing bots from accessing the web site, proactive bot defense protects against these attacks as well.

Working together with other DoS protections, proactive bot defense helps identify and mitigate attacks before they cause damage to the site. This feature inspects most traffic, but requires fewer resources than traditional web scraping and brute force protections. You can use proactive bot defense in addition to the web scraping and brute force protections that are available in ASM security policies. Proactive bot defense is enforced through a DoS profile, and does not require a security policy.

When clients access a protected web site for the first time, the system sends a JavaScript challenge to the browser. Therefore, if you plan to use this feature, it is important that clients use browsers that allow JavaScript.

If the client successfully evaluates the challenge and resends the request with a valid cookie, the system allows the client to reach the server. Requests that do not answer the challenge remain unanswered and are not sent to the server. Requests sent to non-HTML URLs without the cookie are dropped and considered to be bots.

You can configure lists of URLs to consider safe so that the system does not need to validate them. This speeds up access time to the web site. If your application accesses many cross-domain resources and you have a list of those domains, you may want to select an option that validates cross-domain requests to those domains.

Proactive bot defense and CORS

Cross-Origin Resource Sharing (CORS) is a way that web sites can allow resources from another origin access to your site (that is, domain + protocol + port) such as when using AJAX, @font-face, and a few other cases. Proactive Bot Defense blocks CORS requests even for legitimate users. CORS requests are blocked because browsers typically do not include the required cookies when allowing cross-domain requests to prevent session riding by attackers trying to access live sessions and sensitive data from other domains.

Therefore, if you enable Proactive Bot Defense and your web site uses CORS, we recommend that you add the CORS URLs to the proactive bot URL whitelist. Those URLs will not be defended from bots proactively, but they will not be blocked, and will still be protected by other enabled DoS detections and mitigations.

A common type of cross-domain request is when an HTML page references resources from other domains, such as embedded images, style sheets (CSS), and JavaScript. Proactive Bot Defense supports this type of cross-domain request, and you can configure specific domains from which to allow resources in the **Cross-Domain Requests** setting.

About configuring TPS-based DoS protection

When setting up DoS protection, you can configure the system to prevent DoS attacks based on transaction rates (TPS-based anomaly detection). If you use TPS-based anomaly protection, the system detects DoS attacks from the client side using the following calculations:

Transaction rate detection interval

A short-term average of recent requests per second (for a specific URL or from an IP address) that is updated every 10 seconds.

Note: *The averages for IP address and URL counts are done for each site, that is, for each virtual server and associated DoS profile. If one virtual server has multiple DoS profiles (implemented using a local traffic policy), then each DoS profile has its own statistics within the context of the virtual server.*

Transaction rate history interval

A longer-term average of requests per second (for a specific URL or from an IP address) calculated for the past hour that is updated every 10 seconds.

If the ratio of the transaction rate detection interval to the transaction rate during the history interval is greater than the percentage indicated in the **TPS increased by** setting, the system considers the web site to be under attack, or the URL, IP address, or geolocation to be suspicious. In addition, if the transaction rate detection interval is greater than the **TPS reached** setting (regardless of the history interval), then again, the respective URL, IP address, or geolocation is suspicious or the site is being attacked.

Note that TPS-based protection might detect a DoS attack simply because many users are trying to access the server all at once, such as during a busy time or when a new product comes out. In this case, the attack might be a false positive because the users are legitimate. But the advantage of TPS-based DoS protection is that attacks can be detected earlier than when using stress-based protection. So it is important to understand the typical maximum peak loads on your system when setting up DoS protection, and to use the methods that are best for your application.

About configuring stress-based DoS protection

When setting up DoS protection, you can configure the system to prevent DoS attacks based on the server side (stress-based detection). In stress-based detection, it takes a latency increase and at least one suspicious IP address, URL, heavy URL, site-wide entry, or geolocation for the activity to be considered an attack.

Note: *The average latency is measured for each site, that is, for each virtual server and associated DoS profile. If one virtual server has multiple DoS profiles (implemented using a local traffic policy), then each DoS profile has its own statistics within the context of the virtual server.*

Stress-based DoS protection also includes Behavioral DoS. When enabled, the system examines traffic behavior to automatically detect DoS attacks. Behavioral DoS reviews the offending traffic, and mitigates the attack with minimal user intervention required.

Stress-based protection is less prone to false positives than TPS-based protection because in a DoS attack, the server is reaching capacity and service/response time is slow: this is impacting all users. Increased latency can be used as a trigger step for detecting an L7 attack. Following the detection of a significant latency increase, it is important to determine whether you need further action. After examining the increase in the requests per second and by comparing these numbers with past activity, you can identify suspicious versus normal latency increases.

About Behavioral DoS protection

Behavioral DoS (BADoS) provides automatic protection against DDoS attacks by analyzing traffic behavior using machine learning and data analysis. Working together with other BIG-IP® DoS protections, Behavioral DoS examines traffic flowing between clients and application servers in data centers, and automatically establishes the baseline traffic/flow profiles for Layer 7 (HTTP) and Layers 3 and 4.

For example, in the case of a DDoS attack from a botnet, each request may be completely legal but many requests all at once can slow down or crash the server. Behavioral DoS can mitigate the attack by slowing down the traffic no more than necessary to keep the server in good health.

Behavioral DoS continuously monitors server health and loading, by means of a customer feedback loop, to ensure the real-time correlations, and validate server conditions, attacks, and mitigations. Any subsequent anomalies are put on watch, and the system applies mitigations (slowdowns or blocks) as needed.

This is how Behavioral DoS works:

- Learns typical behavior of normal traffic
- Detects an attack based on current conditions (server health)
- Finds behavior anomaly (what and who changed to cause congestion?)
- Mitigates by slowing down suspicious clients
- Improves with experience

You enable Behavioral DoS, which requires minimal configuration, in a DoS profile in the Stress-based detection settings. Because the system is tracking the traffic data, it adapts to changing conditions so there are no thresholds to specify. You set the level of mitigation that you want to occur, ranging from no mitigation (learning only) to aggressive protection (proactive DoS protection). The system can quickly detect Layer 7 DoS attacks, characterize the offending traffic, and mitigate the attack.

You can use a DoS profile that has Behavioral DoS enabled to protect one or, at most, two virtual servers.

About DoS mitigation methods

When setting up either transaction-based or stress-based DoS protection, you can specify *mitigation methods* that determine how the system recognizes and handles DoS attacks. You can use the following methods:

- JavaScript challenges (also called Client-Side Integrity Defense)
- CAPTCHA challenges
- Request blocking (including Rate Limit or Block All)

You can configure the system to issue a JavaScript challenge to analyze whether the client is using a legal browser (that can respond to the challenge) when the system encounters a suspicious IP address, URL, geolocation, or site-wide criteria. If the client does execute JavaScript in response to the challenge, the system purposely slows down the interaction. The Client Side Integrity Defense mitigations are enacted only when the Operation Mode is set to blocking.

Based on the same suspicious criteria, the system can also issue a CAPTCHA (character recognition) challenge to determine whether the client is human or an illegal script. Depending on how strict you want to enforce DoS protection, you can limit the number of requests that are allowed through to the server or block requests that are deemed suspicious.

You can also use can use request blocking in the DoS profile to specify conditions for when the system blocks requests. Note that the system only blocks requests during a DoS attack when the Operation Mode for TPS-based or stress-based detection is set to Blocking. You can use request blocking to rate limit or block all requests from suspicious IP addresses, suspicious countries, or URLs suspected of being under attack. Site-wide rate limiting also blocks requests to web sites suspected of being under attack. If you block all requests, the system blocks suspicious IP addresses and geolocations except those on the whitelist. If you are using rate limiting, the system blocks some requests depending on the threshold detection criteria set in the DoS profile.

The mitigation methods that you select are used in the order they appear on the screen. The system enforces the methods only as needed if the previous method was not able to stem the attack.

About geolocation mitigation

You can mitigate DoS attacks based on geolocation by detecting traffic from countries sending suspicious traffic. This is part of the mitigation methods in the DoS profile for stress-based and TPS-based anomalies, and this method helps protect against unusual activity as follows:

- Geolocation-based Client Side integrity: If traffic from countries matches the thresholds configured in the DoS profile, the system considers those countries suspicious, and sends a JavaScript challenge to each suspicious country.
- Geolocation-based CAPTCHA challenge: If traffic from countries matches the thresholds configured in the DoS profile, the system considers those countries suspicious, and issues a CAPTCHA challenge to each suspicious country.
- Geolocation-based request blocking: The system blocks all, or some, requests from suspicious countries.

In addition, you can add countries to a geolocation whitelist (traffic from these countries is never blocked) and a blacklist (traffic from these countries is always blocked when a DoS attack is detected).

About heavy URL protection

Heavy URLs are URLs that may consume considerable server resources per request. Heavy URLs respond with low latency most of the time, but can easily reach high latency under specific conditions (such as DoS attacks). Heavy URLs are not necessarily heavy all the time, but tend to get heavy especially during attacks. Therefore, low rate requests to those URLs can cause significant DoS attacks and be hard to distinguish from legitimate clients.

Typically, heavy URLs involve complex database queries; for example, retrieving historical stock quotes. In most cases, users request recent quotes with weekly resolution, and those queries quickly yield responses. However, an attack might involve requesting five years of quotes with day-by-day resolution, which requires retrieval of large amounts of data, and consumes considerably more resources.

Application Security Manager™ (ASM) allows you to configure protection from heavy URLs in a DoS profile. You can specify a latency threshold for automatically detecting heavy URLs. If some of the web site's URLs could potentially become heavy URLs, you can manually add them so the system will keep an eye on them, and you can add URLs that should be ignored and not considered heavy.

ASM™ measures the tail latency of each URL and of the whole site for 24 hours to get a good sample of request behavior. A URL is considered *heavy* if its average tail latency is more than twice that of the site latency for the 24-hour period.

About cross-domain requests

Proactive bot defense in a DoS profile allows you to specify which cross-domain requests are legal. *Cross-domain requests* are HTTP requests for resources from a different domain than the domain of the resource making the request.

If your application accesses many cross-domain resources and you have a list of those domains, you can validate cross-domain requests to those domains.

For example, your web site uses two domains, `site1.com` (the main site) and `site2.com` (where resources are stored). You can configure this in the DoS profile by enabling proactive bot defense, choosing one of the **Allowed configured domains** options for the **Cross-Domain Requests** setting, and specifying both of the web sites in the list of related site domains. When the browser makes a request to `site1.com`, it gets cookies for both `site1.com` and `site2.com` independently and simultaneously, and cross domain requests from `site1.com` to `site2.com` are allowed.

If only `site1.com` is configured as a related site domain, when the browser makes a request to `site1.com`, it gets a cookie for `site1.com` only. If the browser makes a cross-domain request to get an image from `site2.com`, it gets a cookie and is allowed only if it already has a valid `site1.com` cookie.

About site-wide DoS mitigation

In order to mitigate highly distributed DoS attacks, such as those instigated using large scale botnets attacking multiple URLs, you can specify when to use site-wide mitigation in a DoS profile. You can configure site-wide mitigation for either TPS-based or stress-based DoS protection. In this case, the whole site can be considered suspicious as opposed to a particular URL or IP address. Site-wide mitigation goes into effect when the system determines that the whole site is experiencing high-volume traffic but is not able to pinpoint and handle the problem.

The system implements site-wide mitigation method only as a last resort because it may cause the system to drop legitimate requests. However, it maintains, at least partially, the availability of the web site, even when it is under attack. When the system applies site-wide mitigation, it is because all other active detection methods were unable to stop the attack.

The whole site is considered suspicious when configured thresholds are crossed, and in parallel, specific IP addresses and URLs could also be found to be suspicious. The mitigation continues until the maximum duration elapses or when the whole site stops being suspicious. That is, there are no suspicious URLs, no suspicious IP addresses, and the whole site is no longer suspicious.

About CAPTCHA challenges in DoS detection

A CAPTCHA (or visual character recognition) challenge displays characters for a client to identify before they can access a web site or application. Whether the client can correctly identify the characters determines whether the client is human or is likely an illegal script. You can configure a CAPTCHA challenge as part of the mitigation policy for TPS-based DoS detection, stress-based DoS detection, or as part of proactive bot defense. If you have configured it, the system a CAPTCHA challenge to suspicious traffic.

The system provides a standard CAPTCHA response that clients will see. You can customize the response if you want.

About DoS protection and HTTP caching

HTTP caching enables the BIG-IP® system to store frequently requested web objects (or static content) in memory to save bandwidth and reduce traffic load on web servers. The Web Acceleration profile has the settings to configure caching.

If you are using HTTP caching along with DoS protection, you need to understand how DoS protection for cached content works. In this case, URLs serving cached content are considered a DoS attack if they exceed the relative **TPS increased by** percentage (and not the explicit **TPS reached** number). Requests to static or cacheable URLs are always mitigated by rate limiting. This is true even during periods of mitigation using client-side integrity or CAPTCHA, and when those mitigations are not only URL-based.

Overview: Preventing DoS attacks on applications

You can configure the Application Security Manager™ to protect against DoS attacks on web applications. Depending on your configuration, the system detects DoS attacks based on transactions per second (TPS) on the client side, stress-based server latency, heavy URLs, geolocation, suspicious browsers, and failed CAPTCHA responses. Behavioral DoS (BADoS), part of stress-based detection, automatically discovers and mitigates DoS attacks using behavioral data.

You configure DoS protection for Layer 7 by creating a DoS profile with Application Security enabled. You then associate the DoS profile with one or more virtual servers representing applications that you want to protect. DoS protection is a system protection that is not part of a security policy.

The main factors in establishing the prevention policy are:

- Attackers: The clients that initiate the actual attacks. They are represented by their IP addresses and the geolocations they come from.
- Servers: The web application servers that are under attack. You can view them site-wide as the pairing of the virtual server and the DoS profile, by the URL, or as a pool member.
- BIG-IP system: The middle tier that detects attacks and associated suspicious entities, then mitigates the attacks, or blocks or drops requests depending on the options you configure in the DoS profile.

Task Summary

Configuring DoS protection for applications

You can configure Application Security Manager™ to protect against and mitigate DoS attacks, and increase system security.

1. On the Main tab, click **Security** > **DoS Protection** > **DoS Profiles**.
   The DoS Profiles list screen opens.
2. Click **Create**.
   The Create New DoS Profile screen opens.
3. In the **Name** field, type the name for the profile, then click **Finished**.
4. In the list of DoS profiles, click the name of the profile you just created, and click the **Application Security** tab.
   This is where you set up application-level DoS protection.
5. In the **General Settings**, for **Application Security**, click **Edit** and select the **Enabled** check box.
   General settings that you can configure are displayed.
6. To configure **Heavy URL Protection**, edit the setting for which URLs to include or exclude, or use automatic detection.

   Another task describes heavy URL protection in more detail.
7. To set up DoS protection based on the country where a request originates, edit the **Geolocations** setting, selecting countries to allow or disallow.
   a) Click **Edit**.
   b) Move the countries for which you want the system to block traffic during a DoS attack into the **Geolocation Blacklist**.
   c) Move the countries that you want the system to allow (unless the requests have other problems) into the **Geolocation Whitelist**.
   d) Use the Stress-based or TPS-based Detection settings to select appropriate mitigations by geolocation in the **How to detect attackers and which mitigation to use** settings.
   e) When done, click **Close**.

8. If you have written an iRule to specify how the system handles a DoS attack and recovers afterwards, enable the **Trigger iRule** setting.
9. To better protect an applications consisting of one page that dynamically loads new content, enable **Single Page Application**.
10. If your application uses many URLs, in **URL Patterns**, you can create logical sets of similar URLs with the varying part of the URL acting like a parameter. Click **Not Configured** and type one or more URL patterns, for example, `/product/*.php`.

    The system then looks at the URL patterns that combine several URLs into one and can more easily recognize DoS attacks, for example, on URLs that might be less frequently accessed by aggregating the statistics from other similar URLs.
11. If you want to use performance acceleration, in **Performance acceleration**, select the TCP fastL4 profile to use as the fast-path for acceleration.

    The profiles listed are those created in **Local Traffic** > **Profiles** > **Protocol** > **Fast L4**.
12. Click **Update** to save the DoS profile.

You have created a DoS profile that provides basic DoS protection including TPS-based detection and heavy URL detection (automatically enabled).

Next, consider configuring additional levels of DoS protection such as stress-based protection, proactive bot defense, and behavioral DoS. Look at the other options available under Application Security and adjust as needed. For example, if using geolocation, use the stress-based or TPS-based detection settings to select appropriate mitigations. Also, you need to associate the DoS profile with a virtual server before it protects against DoS attacks.

Creating a whitelist for DoS protection

You can create a whitelist which is a list of IP addresses that the system does not examine when performing DoS protection.

1. On the Main tab, click **Security** > **DoS Protection** > **DoS Profiles**.
   The DoS Profiles list screen opens.
2. In the list of DoS profiles, click the name of the profile for which you want to specify a whitelist.
   The DoS profile properties tab opens.
3. To omit checking for DoS attacks on certain trusted addresses, edit the **Default Whitelist** setting:
   a) In the Shared Objects frame on the the right side of the screen, next to **Address Lists**, click **+**.
   b) In the Properties panel below, type a name, then one at a time, type trusted IP addresses or subnets that do not need to be examined for DoS attacks, and click **Add**.

   Note: *You can add up to 20 IP addresses.*

   c) When you are done, click **Update**.
   The new whitelist is added to the Address Lists.
   d) To use the new whitelist, after **Default Whitelist**, type the name of the whitelist you added.
4. If you want to create a separate whitelist for HTTP traffic instead of the default whitelist, for **HTTP Whitelist**, select **Override Default** and create a whitelist as you would for the default whitelist.
5. When you are done, click **Update**.

The whitelist you created either for the default or for HTTP is created as a shared object that can be used for all DoS protection. You can use it in any DoS profile including those that contain DoS protection for applications, networks, SIP, and/or DNS.

Using proactive bot defense

For you to use proactive bot defense, client browsers accessing your web site must be able to accept JavaScript. Because this defense mechanism uses reverse lookup, you need to configure a DNS Server (**System** > **Configuration** > **Device** > **DNS**) and a DNS Resolver (**Network** > **DNS Resolvers** > **DNS Resolver List**) for it to work.

You can configure Application Security Manager™ (ASM) to protect your web site against attacks by web robots (called *bots*, for short) before the attacks occur. Proactive bot defense checks all traffic (except whitelisted URLs) coming to the web site, not simply suspicious traffic. This DoS protection uses a set of JavaScript evaluations and bot signatures to make sure that browsers visiting your web site are legitimate.

Important: *Proactive bot defense has limitations if your web site uses Cross-Origin Resource Sharing (CORS), for example, with AJAX requests.*

1. On the Main tab, click **Security** > **DoS Protection** > **DoS Profiles**.
   The DoS Profiles list screen opens.
2. Click the name of an existing DoS profile (or create a new one, then open it), and click the **Application Security** tab.
3. On the left, under Application Security, click **General Settings**, and ensure that **Application Security** is enabled.
   The screen displays additional settings.
4. On the left, click **Proactive Bot Defense**.
5. Set the **Operation Mode** to specify when to implement proactive bot defense.

Option	Description
During Attacks	Checks all traffic during a DoS attack, and prevents detected attacks from escalating.
Always	Checks all traffic at all times, and prevents DoS attacks from starting.

   Important: *If you enable Proactive Bot Defense and your web site uses CORS (Cross-Origin Resource Sharing), we recommend that you add the CORS URLs to the proactive bot URL whitelist.*

   The system enables Bot Signatures to enforce Proactive Bot Defense. By default, the system blocks requests from highly suspicious browsers and displays a default CAPTCHA (or visual character recognition) challenge to browsers that are suspicious.
6. By default, the **Block requests from suspicious browsers** setting and check boxes are enabled. If you do not want to block suspicious browsers or send a CAPTCHA challenge, you can clear the **Block Suspicious Browsers** or **CAPTCHA Challenge** check boxes.

   You can also change the CAPTCHA response by clicking **CAPTCHA Settings**. (Another task explains how to configure CAPCHA when setting up DoS protection.)
7. In the **Grace Period** field, type the number of seconds to wait before the system blocks suspected bots.

   The default value is **300** seconds.

   The grace period allows web pages (including complex pages such as those which include images, JS, and CSS) the time to be recognized as non-bots, receive validation, and completely load without unnecessarily dropping requests.

   The grace period begins after the client is validated, a configuration change occurs, or when proactive bot defense starts as a result of a detected DoS attack or high latency.

8. Using the **Cross-Domain Requests** setting, specify how the system validates cross-domain requests (such as requests for non-HTML resources like embedded images, CSS style sheets, XML, JavaScript, or Flash).

   Cross-domain requests are requests with different domains in the Host and Referrer headers.

Option	Description
Allow all requests	Allows requests arriving to a non-HTML URL referred by a different domain and without a valid cookie if they pass a simple challenge. The system sends a challenge that tests basic browser capabilities, such as HTTP redirects and cookies.
Allow configured domains; validate in bulk	Allows requests to other related internal or external domains that are configured in this section, and validates the related domains in advance. The requests to related site domains must include a valid cookie from one of the site domains; the external domains are allowed if they pass a simple challenge. Choose this option if your web site does not use many domains, and then include them all in the lists below. Also, if your website uses CORs, select this option and then specify the WebSocket domain in the Related Site Domains list.
Allow configured domains; validate upon request	Allows requests to other related internal or external domains that are configured in this section. The requests to related site domains must include a valid cookie from the main domain; the external domains are allowed if they pass a simple challenge. Choose this option if your web site uses many domains, and include the main domain in the list below.

9. If you selected one of the **Allow configured domains** options in the last step, you need to add **Related Site Domains** that are part of your web site, and **Related External Domains** that are allowed to link to resources in your web site.
10. In the **URL Whitelist** setting, add the resource URLs for which the web site expects to receive requests and that you want the system to consider safe.

    Type URLs in the form `/index.html`, then click **Add.**. Wildcards are supported.

    Tip: *If your web site uses CORS, add the CORS URLs to the whitelist, otherwise, they will be blocked.*

    The system does not perform proactive bot defense on requests to the URLs in this list.
11. Click **Update** to save the DoS profile.

You have now configured proactive bot defense which protects against DDoS, web scraping, and brute force attacks (on the virtual servers that use this DoS profile). By creating a bot defense logging profile, you can view a Bot Defense event log at **Security** > **Event Logs** > **Bot Defense**.

The system sends a JavaScript challenge to traffic accessing the site for the first time. Legitimate traffic answers the challenge correctly, and resends the request with a valid cookie; then it is allowed to access the server. The system drops requests sent by browsers that do not answer the system's initial JavaScript challenge (considering those requests to be bots). The system also automatically enables bot signatures and blocks bots known to be malicious.

If proactive bot detection is always running, ASM™ filters out bots before they manage to build up an attack on the system and cause damage. If using proactive bot defense only during attacks, once ASM detects a DoS attack, the system uses proactive bot defense for the duration of the attack.

Proactive bot defense is used together with the active mitigation methods specified in TPS- and stress-based detection. Any request that is not blocked by the active mitigation method still has to pass the proactive bot defense mechanism to be able to reach the server (unless it is on the URL whitelist). Proactive bot defense blocks requests to CORS (Cross-Origin Resource Sharing) URLs not on the URL whitelist.

Configuring bot defense logging

Before beginning to configure bot defense logging, ensure that you have configured remote logging to Splunk for your system. Both the F5 DevCentral and Splunk websites have information on how to configure BIG-IP to send logs to a Splunk platform. Local logging is not recommended.

1. On the **Main** tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profile screen opens.
2. Click the name of an existing logging profile (or create a new one, then open it).
   The Logging Profile Properties screen opens.
3. Enable **Bot Defense**.
   The Bot Defense tab opens.
4. From the **Bot Defense** tab, select your preconfigured **Remote Publisher** from the drop down list.
5. Enable the log details you want to capture.
6. Click **Update** to save the logging profile.
7. On the Main tab, click **Local Traffic** > **Virtual Servers** > **Virtual Server List**.
8. Select the virtual server to associate the bot defense logging profile to.
   The Properties tab opens.
9. Click the **Security** > **Policies** tab.
10. Enable **DoS Protection Profile**.
11. In the **Log Profile** section, select the bot defense profile from the ui**Available** list and move it to the **Selected** list.
12. Click **Update** to save the Policy Settings.

You can view the bot defense logs by navigating to **Security** > **Event Logs** > **Bot Defense** > **Requests**.

Configuring bot signature checking

If you need to create custom bot signatures and categories for your application, you should do this before configuring bot signature checking. Navigate to **Security** > **Options** > **DoS Protection** > **Bot Signatures List**. Otherwise, you can use the system-supplied bot signatures and categories listed in the same place.

Because this defense mechanism uses reverse lookup, you need to configure a DNS Server (**System** > **Configuration** > **Device** > **DNS**) and a DNS Resolver (**Network** > **DNS Resolvers** > **DNS Resolver List**) for it to work.

Bot signature checking is typically used with proactive bot defense (and is enabled by default when you use proactive bot defense). The system performs bot signature checking, which identifies known bots as legitimate or malicious based on their HTTP characteristics. You can specify whether to ignore, report, or block certain categories of malicious or benign bots. You can also disable specific bot signatures, if needed.

1. On the Main tab, click **Security** > **DoS Protection** > **DoS Profiles**.
   The DoS Profiles list screen opens.
2. Click the name of an existing DoS profile (or create a new one, then open it), and click the **Application Security** tab.
3. On the left, under Application Security, click **General Settings**, and ensure that **Application Security** is enabled.
   The screen displays additional settings.
4. On the left, click **Bot Signatures** to display the settings.
5. For the **Bot Signature Check** setting, select **Enabled** if it is not already selected.

6. In the **Bot Signature Categories** field, for each category of bots, both malicious and benign, select the action to take when a request matches a signature in that category.

Option	Action
None	Ignore requests in this category.
Report	Log requests in this category.
Block	Block and report requests in this category.

   You can select one action for all malicious or all benign categories, or have different actions for separate categories.

   Note:

   These settings override the **Proactive Bot Defense** settings. For example, requests from bots in any category, if set to **Block**, are always blocked.

7. If certain signatures need to be disabled, in the **Bot Signatures List**, move the signatures to the **Disabled Signatures** list.
8. Click **Update** to save the DoS profile.

You have specified how to perform bot signature checking on your system. By comparing the bot signatures with requests, the system can identify those made by different categories of bots and will ignore, report, or block requests from bots it discovers.

If using bot signature checking, you will want to keep the signatures up to date. You can configure bot signatures (and all other signatures) to be updated automatically or update them manually using the Security Updates feature. A security update downloads the latest new and updated bot signatures and attack signatures.

Configuring TPS-based DoS detection

You can configure Application Security Manager™ to mitigate DoS attacks based on transaction rates using TPS-based DoS protection.

1. On the Main tab, click **Security** > **DoS Protection** > **DoS Profiles**.
   The DoS Profiles list screen opens.
2. Click the name of an existing DoS profile (or create a new one, then open it), and click the **Application Security** tab.
3. On the left, under Application Security, click **General Settings**, and ensure that **Application Security** is enabled.

   If **Application Security** is disabled, click **Enabled**.

   The screen displays additional settings.
4. On the left, under Application Security, click **TPS-based Detection**.
   The screen displays TPS-based DoS Detection settings.
5. Click **Edit All**.

   You can also edit each setting separately instead of editing them all at once.

   The screen opens the settings for editing.
6. For **Operation Mode**, select the option to determine how the system reacts when it detects a DoS attack.

Option	Description
Transparent	Displays data about DoS attacks on the DoS reporting screens, but does not block requests, or perform any of the mitigations.

Option	Description
Blocking	Applies the necessary mitigation steps to suspicious IP addresses, geolocations, URLs, or the entire site. Also displays information about DoS attacks on the DoS reporting screens.

Select **Off** to turn this type of DoS Detection off.

The screen displays additional configuration settings when you select an operation mode.

7. For **Thresholds Mode**, select whether to let the system automatically determine thresholds (**Automatic**) or to set the threshold values manually (**Manual**) for the DoS profile.

   If you choose to set the values manually, more fields are shown in the **How to detect attackers and which mitigation to use** setting, and you can adjust the threshold values. The default values are reasonable for most installations. If using automatic thresholds, the system sets the values using a wide range to begin with, then calculates the values using 7 days of historical data and sets threshold values to the highest levels during normal activity (to minimize false positives). The system updates thresholds every 12 hours.

8. For **How to detect attackers and which mitigation to use**, specify how to identify and stop DoS attacks. By default, source IP addresses and URLs are used to detect DoS attacks. You can specify other detection methods, and, if setting thresholds manually, adjust the thresholds for each of the settings as needed.

Option	Description
By Source IP	Specifies conditions for when to treat an IP address as an attacker. For automatic thresholds, one threshold is used for all source IP addresses.
By Device ID	Specifies conditions for when to treat a device as an attacker. For automatic thresholds, one threshold is used for all device IDs.
By Geolocation	Specifies when to treat a particular country as an attacker. If using automatic thresholds, the system calculates thresholds for the top 20 geolocations, setting different thresholds for every hour of the day. Thus, thresholds calculated at 9:00AM are based on data from 8:00-9:00AM, and are used at 8:00AM next day.
By URL	Specifies when the system treats a URL as under attack. For automatic thresholds, one threshold is used for all URLs. (Heavy URLs are not included in the calculations.)
Site Wide	Specifies conditions for how to determine when the entire web site is under attack. For automatic thresholds, one threshold value is used for the entire site.

At least one mitigation method must be selected before you can edit the detection settings. If the specified thresholds in the settings are reached, the system limits the number of requests per second to the history interval and uses the selected mitigation methods described here.

Option	Description
Client Side Integrity Defense	Sends a JavaScript challenge to determine whether the client is a legal browser or an illegal script. Only used when the **Operation Mode** is set to **Blocking**.
CAPTCHA Challenge	Issues a CAPTCHA challenge to the traffic identified as suspicious by source IP address, geolocation, URL, or site wide.
Request Blocking	Specifies how and when to block (if the operation mode is set to **Blocking**) or report (if the operation mode is set to **Transparent**)

Option	Description
	suspicious requests. Select **Block All** to block all suspicious requests or **Rate Limit** to reduce the number of suspicious requests.

9. For the **Prevention Duration** setting, specify the time spent in each mitigation step until deciding to move to the next mitigation step.

Option	Description
Escalation Period	Specifies the minimum time spent in each mitigation step before the system moves to the next step when preventing attacks against an attacker IP address or attacked URL. During a DoS attack, the system performs attack prevention for the amount of time configured here for the mitigation methods that are enabled. If after this period the attack is not stopped, the system enforces the next enabled prevention step. Type a number between `1` and `3600`. The default is `120` seconds.
De-escalation Period	Specifies the time spent in the final escalation step until retrying the steps using the mitigation methods that are enabled. Type a number (greater than the escalation period) between `0` (meaning the steps are never retried) and `86400` seconds. The default value is `7200` seconds (2 hours).

DoS mitigation is reset after 2 hours, even if the detection criteria still hold, regardless of the value set for the **De-escalation Period**. If the attack is still taking place, a new attack occurs and mitigation starts over, retrying all the mitigation methods. If you set the **De-escalation Period** to less than 2 hours, the reset occurs more frequently.

10. Click **Update** to save the DoS profile.

You have now configured a DoS profile to prevent DoS attacks based on the client side (TPS-based detection). When the system receives too many requests per second for a source IP address, device ID, URL, or site wide, it is considered suspicious. The attack starts if the system detects at least one suspicious entity. The attack ends when there are no suspicious entities for a period of two minutes.

Next, you need to associate the DoS profile with the application's virtual server. You also have the option of configuring stress-based detection, heavy URL protection, or proactive bot defense in your DoS profile.

Configuring behavioral & stress-based DDoS protection

You can configure Application Security Manager™ to mitigate Layer 7 DDoS attacks based on server latency and traffic behavior. Behavioral DDoS protection is based on continuous machine learning of traffic and flow characteristics, and detects attacks very quickly.

1. On the Main tab, click **Security** > **DoS Protection** > **DoS Profiles**.
   The DoS Profiles list screen opens.
2. Click the name of an existing DoS profile (or create a new one, then open it), and click the **Application Security** tab.
3. On the left, under Application Security, click **General Settings**, and ensure that **Application Security** is enabled.
   The screen displays additional settings.
4. On the left, under Application Security, click **Behavioral & Stress-based Detection**.
   The screen displays Behavioral & Stress-based DoS Detection settings.
5. Click **Edit All**.

   You can also edit each setting separately instead of editing them all at once.

   The screen opens the settings for editing.

6. For **Operation Mode**, select the option to determine how the system reacts when it detects a DoS attack.

Option	Description
Transparent	Displays data about DoS attacks on the DoS reporting screens, but does not block requests, or perform any of the mitigations.
Blocking	Applies the necessary mitigation steps to suspicious IP addresses, geolocations, URLs, or the entire site. Also displays information about DoS attacks on the DoS reporting screens.

   Select **Off** to turn this type of DoS Detection off.

   The screen displays additional configuration settings when you select an operation mode.

7. For **Thresholds Mode**, select whether to let the system automatically determine thresholds (**Automatic**) or to set the threshold values manually (**Manual**) for the DoS profile.

   If you choose to set the values manually, more fields are shown in the **Stress-based Detection and Mitigation** setting, and you can adjust the threshold values. The default values are reasonable for most installations. If using automatic thresholds, the system sets the values using a wide range to begin with, then calculates the values using 7 days of historical data and sets threshold values to the highest levels during normal activity (to minimize false positives). Thereafter, the system updates thresholds every 12 hours.

8. For **Stress-based Detection and Mitigation**, specify how to identify and stop DoS attacks. By default, source IP addresses and URLs are enabled to detect DoS attacks. You can specify other detection methods, and, if setting thresholds manually, adjust the thresholds for each of the settings as needed.

Option	Description
By Source IP	Specifies conditions for when to treat an IP address as an attacker. The system calculates one automatic threshold for the most accessed source IP addresses, and another threshold for the rest.
By Device ID	Specifies conditions for when to treat a device as an attacker. For automatic thresholds, one threshold is calculated for highly accessed device IDs, and another for the rest.
By Geolocation	Specifies when to treat a particular country as an attacker. If using automatic thresholds, the system calculates thresholds for the top 20 geolocations, setting different thresholds for every hour of the day. Thus, thresholds calculated at 9:00AM are based on data from 8:00-9:00AM, and are used at 8:00AM next day.
By URL	Specifies when the system treats a URL as under attack. For automatic thresholds, one threshold is calculated for highly accessed URLs, and another for the rest. (Heavy URLs are not included in the calculations.)
Site Wide	Specifies conditions for how to determine when the entire web site is under attack. For automatic thresholds, one threshold is used sitewide.

   At least one mitigation method must be selected before you can edit the detection settings. If the specified thresholds in the settings are reached, the system limits the number of requests per second to the history interval and uses the selected mitigation methods described here. These methods do not apply to Behavioral DoS.

Option	Description
Client Side Integrity Defense	Sends a JavaScript challenge to determine whether the client is a legal browser or an illegal script. Only used when the **Operation Mode** is set to **Blocking**.
CAPTCHA Challenge	Issues a CAPTCHA challenge to the traffic identified as suspicious by source IP address, geolocation, URL, or site wide.
Request Blocking	Specifies how and when to block (if the operation mode is set to **Blocking**) or report (if the operation mode is set to **Transparent**) suspicious requests. Select **Block All** to block all suspicious requests or **Rate Limit** to reduce the number of suspicious requests.

9. For the **Behavioral Detection and Mitigation** settings, specify how to mitigate DDoS attacks discovered based on behavior.

Option	Description
Bad actors behavior detection	Lets the system identify IP addresses of bad actors by examining traffic behavior and anomaly detection.
Request signatures detection	Examines requests and creates behavioral signatures describe patterns found in attacks the system has identified. Select **Use approved signatures only** if you want to verify that the system-generated signatures are valid before letting the system use them.
Mitigation	Specifies the level of mitigation to perform for attacks discovered using behavioral DoS. • **Conservative Protection**: If **Bad actors behavior detection** is enabled, slows down and rate limits requests from anomalous IP addresses based on anomaly detection confidence and server health. If **Request signatures detection** is enabled, blocks requests that match behavioral signatures. • **Standard Protection**: If **Bad actors behavior detection** is enabled, slows down requests from anomalous IP addresses based on its anomaly detection confidence and server health. Rate limits requests from anomalous IP addresses and, if necessary, rate limits all requests based on server health. Limits the number of concurrent connections from anomalous IP addresses and, if necessary, limits the number of all concurrent connections based on server health. If **Request signatures detection** is enabled, blocks requests that match behavioral signatures. • **Aggressive Protection**: If **Bad actors behavior detection** is enabled, does all that standard protection does plus it proactively performs all protection actions (even before an attack). Increases the impact of the protection techniques. If **Request signatures detection** is enabled, blocks requests that match behavioral signatures. Increases the impact of blocked requests. • **No Mitigation**: Learns and monitors traffic behavior, but takes no action.

10. For the **Prevention Duration** setting, specify the time spent in each mitigation step until deciding to move to the next mitigation step.

Option	Description
Escalation Period	Specifies the minimum time spent in each mitigation step before the system moves to the next step when preventing attacks against an attacker IP address or attacked URL. During a DoS attack, the system performs attack prevention for

Option	Description
	the amount of time configured here for the mitigation methods that are enabled. If after this period the attack is not stopped, the system enforces the next enabled prevention step. Type a number between `1` and `3600`. The default is `120` seconds.
De-escalation Period	Specifies the time spent in the final escalation step until retrying the steps using the mitigation methods that are enabled. Type a number (greater than the escalation period) between `0` (meaning the steps are never retried) and `86400` seconds. The default value is `7200` seconds (2 hours).

DoS mitigation is reset after 2 hours, even if the detection criteria still hold, regardless of the value set for the **De-escalation Period**. If the attack is still taking place, a new attack occurs and mitigation starts over, retrying all the mitigation methods. If you set the **De-escalation Period** to less than 2 hours, the reset occurs more frequently.

11. Click **Update** to save the DoS profile.

You have now configured a DoS profile to prevent DoS attacks automatically based on server health and/or Behavioral DoS. The BIG-IP® system monitors server health and estimates the server load based on Layer 7 statistics including TPS, pending transactions, request drop rate, and so on. If the system detects potential attack conditions, the mitigation starts working (depending on the level of behavioral protection you selected) seconds after an attack begins.

***Note:** If using stress-based or behavioral DoS protection, the system may falsely detect an attack in the event of a runtime failure (such as a backend server being down) or a configuration issue (such as the system having no pool or the pool having no pool members).*

The mitigation process starts with the list of suspicious IP addresses and slows down suspicious clients. The system may also perform ingress rate shaping. The suspicious clients are tagged as a result of the Layer 7 behavioral analysis.

Next, associate the DoS profile with the application's virtual server. You also have the option of configuring TPS-based detection, proactive bot defense, or heavy URL protection in your DoS profile.

Configuring heavy URL protection

To use heavy URL protection, F5 recommends that you configure stress-based anomaly settings in the DoS profile. That way the system can detect low-volume attacks on heavy URLs when no other high-volume attacks are underway. Also, you must enable at least one of the URL-based prevention policy methods in the TPS-based Anomaly or stress-based Anomaly settings in the DoS profile.

You can configure Application Security Manager™ (ASM) to prevent DoS attacks on heavy URLs. Heavy URLs are URLs on your application web site that may consume considerable resources under certain conditions. By tracking URLs that are potentially heavy, you can mitigate DoS attacks on these URLs before response latency exceeds a specific threshold.

1. On the Main tab, click **Security** > **DoS Protection** > **DoS Profiles**.
   The DoS Profiles list screen opens.
2. Click the name of an existing DoS profile (or create a new one, then open it), and click the **Application Security** tab.
3. On the left, under Application Security, click **General Settings**, and ensure that **Application Security** is enabled.
   The screen displays additional settings.
4. In the General Settings, next to **Heavy URL Protection**, click **Edit**.

5. To have the system automatically detect heavy URLs, select **A URL is considered heavy if its portion of transactions with latency above this threshold is higher than usual for this site**, and adjust the latency threshold if necessary.

   The default value is `1000` milliseconds.

   The system detects heavy URLs by measuring the latency tail ratio, which is the number of transactions whose latency is consistently greater than the threshold.
6. If you expect certain URLs to be heavy (have high latency) at times, add them to the **Configure a list of Heavy URLs** setting:
   a) Type each URL in the form `/query.html`. The URLs in this list may include wildcards, such as `/product/*`.
   b) Type the threshold in milliseconds at which point you want the URL to be considered heavy.
   c) Click **Add**, adding as many URLs as you need to.

   If you are not sure which URLs to add to the Heavy URLs list, leave this setting unconfigured and let the system automatically detect heavy URLs.

   If you want to add a wildcard URL to the heavy URL list, you also must add the wildcard URL to the **URL Patterns** field on this screen. A wildcard not added to the URL Patterns will not function as a wildcard.
7. In the **Configure a list of URLs which are excluded from being automatically detected as Heavy URLs** setting, type the URLs not to consider heavy, and click **Add**.

   The URLs in this list may include wildcards, such as `/product/*` .
8. Click **Update** to save the DoS profile.

You have now configured a DoS profile that includes heavy URL protection. Heavy URLs are detected based on reaching higher latency under certain conditions. ASM tracks the probability distribution of server latency, which is called heavy tailed.

To validate automatic detection, you can view the URL Latencies report (**Security** > **Reporting** > **DoS** > **URL Latencies**) periodically to check that the latency threshold that you used is close to the value in the latency histogram column for all traffic. You should set the latency threshold so that approximately 95% of the requests for the virtual server have lower latency.

By reviewing the URL Latencies report and sorting the URLs listed by latency, you can make sure that the URLs that you expect to be heavy are listed in the DoS profile. Also, if the system detects too many (or too few) heavy URLs, you can increase (or decrease) the latency threshold.

Recording traffic during DoS attacks

If you have DoS protection enabled, you can configure the system to record traffic during DoS attacks. By reviewing the recorded traffic in the form of a TCP dump, you can diagnose the attack vectors and attackers, observe whether and how the attack was mitigated, and determine whether you need to change the DoS protection configuration.

1. On the Main tab, click **Security** > **DoS Protection** > **DoS Profiles**.
   The DoS Profiles list screen opens.
2. Click the name of an existing DoS profile (or create a new one, then open it), and click the **Application Security** tab.
3. On the left, under Application Security, click **General Settings**, and ensure that **Application Security** is enabled.
   The screen displays additional settings.
4. On the left, under Application Security, click **Record Traffic**.
5. For **Record Traffic During Attacks**, click **Edit**, then select the **Enabled** check box.
   The screen displays additional configuration settings.

6. For **Maximum TCP Dump Duration**, click **Edit**, then type the maximum number of seconds (from 1 - 300) for the system to record traffic during a DoS attack.

   The default value is `30` seconds.
7. For **Maximum TCP Dump Size**, type the maximum size (from 1 - 50) allowed for the TCP dump.

   When the maximum size is reached, the dump is complete. The default value is `10` MB.
8. For **TCP Dump Repetition**, specify how often to perform TCP dumps during a DoS attack:
   - To record traffic once during an attack, select **Dump once per attack**.
   - To record traffic periodically during an attack, select **Repeat dump after** and type the number of seconds (between 1 - 3600) for how long to wait after completing a TCP dump before starting the next one.
9. Click **Update** to save the DoS profile.

When the system detects a DoS attack, it performs a TCP dump to record the traffic on the virtual server where the attack occurred. The files are located on the system in `/shared/dosl7/tcpdumps`. The name of the file has the format: `<yyyy_mm_dd_hh:mm:ss>-<attack_ID>-<seq_num>.pcap`, including the time the dump started, the ID of the attack in logs and reports, and the number of the TCP dump since the attack started. If traffic being recorded is SSL traffic, it is recorded encrypted.

If working with F5 support, you can collect the TCP dump files into a QuickView file so that support personnel can help determine the cause of the DoS attack, and recommend ways of preventing future attacks.

Configuring CAPTCHA for DoS protection

You can configure a CAPTCHA challenge as part of the mitigation policy for TPS-based DoS detection, behavioral & stress-based DoS detection, or as part of proactive bot defense. A CAPTCHA (or visual character recognition) challenge determines whether the client is human or an illegal script.

1. On the Main tab, click **Security** > **DoS Protection** > **DoS Profiles**.
   The DoS Profiles list screen opens.
2. Click the name of an existing DoS profile (or create a new one, then open it), and click the **Application Security** tab.
3. On the left, under Application Security, click **General Settings**, and ensure that **Application Security** is enabled.
   The screen displays additional settings.
4. On the left, under Application Security, select an option to configure TPS-based, behavioral & stress-based, or proactive bot defense, and select CAPTCHA as one of the mitigation methods.
   a) For **TPS-based Detection**, in the **How to detect attackers and which mitigation to use** setting, edit the source IP, device ID, geolocation, URL, or site-wide mitigation, and select **CAPTCHA Challenge**.
   b) For **Behavioral & Stress-based Detection**, in the **Stress-based Detection and Mitigation** setting, edit the source IP, device ID, geolocation, URL, or site-wide mitigation, and select **CAPTCHA Challenge**.
   c) For **Proactive Bot Defense**, in the **Block requests from suspicious browsers** setting, select **CAPTCHA Challenge** to challenge a suspected bot.
5. To customize the CAPTCHA response that the system sends as a challenge to suspicious users, click **CAPTCHA Settings**.

   The **CAPTCHA Settings** link is only available after you select a CAPTCHA challenge.

   The Application Security General Settings area opens and displays the CAPTCHA Response.
6. In the **CAPTCHA Response** setting, specify the text the system sends as a challenge to users.

***Note:** This setting appears only if one or more of the CAPTCHA Challenge options is selected.*

a) From the **First Response Type** list, select **Custom**.
b) Edit the text (HTML) in the **First Response Body** field.

You can use the following variables within the challenge or response.

Variable	Use
`%DOSL7.captcha.image%`	Displays the CAPTCHA image in data URI format.
`%DOSL7.captcha.change%`	Displays the change CAPTCHA challenge icon.
`%DOSL7.captcha.solution%`	Displays the solution text box.
`%DOSL7.captcha.submit%`	Displays the **Submit** button.

c) Click **Show** to see what it looks like.

7. In the **CAPTCHA Response** setting, specify the text the system sends to users if they fail to respond correctly to the CAPTCHA challenge.

a) From the **Failure Response Type** list, select **Custom** if you want to change the text.
b) If customizing the text, edit the text in the **Failure Response Body** field.

You can use the same variables in the text to send a second challenge.

c) Click **Show** to see what it looks like.

8. Click **Update** to save the DoS profile.

You have now configured a CAPTCHA challenge for potential DoS attackers that helps with filtering out bots. The system sends a character recognition challenge only on the first request of a client session. If it is solved correctly, the request is sent to the server. Subsequent requests in the session do not include the challenge. If the client fails the first challenge, the CAPTCHA response is sent. If that also fails, the client is handled according to the mitigation methods selected in the DoS profile.

Associating a DoS profile with a virtual server

You must first create a DoS profile separately, to configure denial-of-service protection for applications, the DNS protocol, or the SIP protocol. For application-level DoS protection, the virtual server requires an HTTP profile (such as the default http).

You add denial-of-service protection to a virtual server to provide enhanced protection from DoS attacks, and track anomalous activity on the BIG-IP® system.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
The Virtual Server List screen opens.

2. Click the name of the virtual server you want to modify.

3. On the menu bar, from the Security menu, choose Policies.

4. To enable denial-of-service protection, from the **DoS Protection Profile** list, select **Enabled**, and then, from the **Profile** list, select the DoS profile to associate with the virtual server.

5. Click **Update** to save the changes.

DoS protection is now enabled, and the DoS Protection profile is associated with the virtual server.

Implementation Result

When you have completed the steps in this implementation, you have configured the Application Security Manager™ (ASM) to protect against L7 DoS attacks. If using proactive bot defense, ASM™ protects against DDoS, web scraping, and brute force attacks (on the virtual servers that use this DoS profile) before the attacks can harm the system. Depending on the configuration, the system may also detect DoS attacks based on transactions per second (TPS) on the client side, server latency, or both.

In TPS-based detection mode, if the ratio of the transaction rate during the history interval is greater than the TPS increased by percentage, the system considers the URL to be under attack, the IP address or country to be suspicious, or possibly the whole site to be suspicious.

In stress-based detection mode, if there is a latency increase and at least one suspicious IP address, country, URL, or heavy URL, the system considers the URL to be under attack, the IP address or country to be suspicious, or possibly the whole site to be suspicious.

If you enabled heavy URL protection, the system tracks URLs that consume higher than average resources and mitigates traffic that is going to those URLs.

If you chose the blocking operation mode, the system applies the necessary mitigation steps to suspicious IP addresses, URLs, or geolocations, or applies them site-wide. If using the transparent operation mode, the system reports DoS attacks but does not block them.

If you are using iRules® to customize reaction to DoS attacks, when the system detects a DoS attack based on the configured conditions, it triggers an iRule and responds to the attack as specified in the iRule code.

After traffic is flowing to the system, you can check whether DoS attacks are being prevented, and investigate them by viewing DoS event logs and reports.